TechTips Newsletter

tech hero

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

December 2020

This monthly publication provided courtesy of Richard Lynn, VP of Sales and Marketing Tech Hero

Our Mission

To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

Russia Suspected In Major Cyberattack On U.S. Government

Russian hackers working for the Kremlin are believed to be behind breaches of U.S. government computer systems at the departments of Treasury, Commerce and Homeland Security that may have lasted months before they were discovered, according to U.S. officials and media reports.

The hackers reportedly broke into the email systems at the government departments, but the full extent of the breach was not immediately clear as U.S. officials scrambled to make an assessment. There are concerns that hackers may have penetrated other government departments and perhaps many private companies as well.

Continued on next page...

The Commerce Department, the National Security Council and the Department of Homeland Security all acknowledged the intrusion in brief statements but provided no details.

"We can confirm there has been a breach in one of our bureaus," the Commerce Department said.

"We have been working closely with our agency partners regarding recently discovered activity on government networks," said NSC spokesman John Ullyot.

The U.S. government did not name Russia or any other actor as being responsible.

Reuters first reported the story on Sunday, and subsequent reports identified Russia's foreign intelligence service, the SVR, as the most likely culprit.

Russia's SVR, the rough equivalent to the CIA in the U.S., was blamed for major hacks in 2014-15 that involved unclassified email systems at the White House, State Department and the Joint Chiefs of Staff.

Russia on Monday denied any involvement in the latest reported breach.

Emergency directive

Meanwhile, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), which is part of Homeland Security, issued an emergency directive calling on all federal civilian agencies to review their computer networks for signs of the compromise. The statement also said agencies should disconnect from SolarWinds Orion products immediately.

SolarWinds has government contracts, including with the military and intelligence services, and also works with many large private companies. The attackers are believed to have used a "supply chain attack" method that embeds malicious code into legitimate software updates.

"The compromise of SolarWinds' Orion Network Management Products poses unacceptable risks to the security of federal networks," CISA's acting Director Brandon Wales said in a statement. "Tonight's directive is intended to mitigate potential compromises within federal civilian networks, and we urge all our partners — in the public and private sectors — to assess their exposure to this compromise."

SolarWinds, based in Austin, Texas, put out its own statement saying it was aware that its systems were experiencing a "highly sophisticated, manual supply chain attack" on specific versions of its Orion platform software released between March and June of this year.

"We have been advised this attack was likely conducted by an outside nation-state and intended to be a narrow, extremely targeted, and manually executed attack, as opposed to a broad, system-wide attack," the company said.

Kevin Thompson, SolarWinds' president and CEO, said the company was working with the FBI, the U.S. intelligence community and other law enforcement agencies to investigate.

— *NPR's Jaclyn Diaz reporting (NPR's national security correspondent Greg Myre contributed to this report)*

vmware PARTNER

PROFESSIONAL SOLUTION PROVIDER

Free Consultation to review your VMware Licensing!

Contact your Tech Hero sales representative to schedule a FREE review of your VMware licensing.

Find out ways to save money, ways to receive free upgrades, and a better understanding on the VMware license models.

tech hero

1-(800) 900-TECH (option 2)

Sales@TechHero.com

Home Depot settles with numerous states following data breach...

Back in 2014, Home Depot experienced what many cybersecurity experts considered the largest retail card data breach in history. In the breach, 56 million debit and credit cards were accessed by hackers and a class-action lawsuit was subsequently filed by affected customers. The consumer lawsuit resulted in a payout of around $19.5 million, with $13 million being set aside for direct reimbursement and $6.5 million being used to provide identity protection services at no charge to the customers suing. This suit was concluded in 2016, but Home Depot was far from out of the woods on this issue.

According to a recent Reuters report published in late November 2020, Home Depot also reached a settlement with numerous states in the U.S. The report states that Home Depot paid the attorney general offices of 46 states and Washington D.C. $17.5 million for negligence shown at the time of the breach. Much of the case hinges on poor encryption standards that allowed hackers to access self-checkout point-of-sale (POS) systems.

The investigation that resulted in the settlement was led by the attorneys general of Connecticut, Illinois, and Texas. As quoted by Reuters, Connecticut Attorney General William Tong said ted that any company collecting sensitive data (such as credit and debit card information) “have an obligation to protect that information from unlawful use or disclosure,” and that “Home Depot failed to take those precautions.” Home Depot still denies any wrongdoing in the incident, but they also state that they have made changes to their cybersecurity since the incident.

Continued on next page...

In a statement to the press, Home Depot asserted that they "invested heavily to further secure our systems." Home Depot is also quoted as saying "we're glad to put this matter behind us."

While the Home Depot data breach case is now over, it serves as a lesson to any company handling sensitive data. If you invest in cybersecurity, it will pay dividends for you. By protecting consumer data, companies will not have to worry about legal action later that tarnishes their reputation and results in massive payouts (either through settlement or fines). —*Derek Kortepeter for Techgenix*

Client Spotlight

20 years of providing the highest quality meats at shopping-list friendly prices makes Colorado Choice Distributors the premiere selection for six pack variety steaks, chicken, pork and seafood.

The patrons at your table deserve the best quality, and you deserve the best price. When you want a cut above the rest, you want Colorado Choice Distributors.

tech hero

Cloud Portal

Did you know about our new Cloud Portal? This new tool will allow you to open tickets directly with us here at Tech Hero at the click of a button!

To try it out, just go down to your system tray and look for the small blue IT icon. After you've double clicked on it you will need to sign in (You will only need to do this once!)

Once you are in you can click around explore the software.

If you have any questions, feel free to reach out to us at the number below!

(800) 900-TECH x2

OFFICE 365 IS NOW MICROSOFT 365: EVERYTHING YOU NEED TO KNOW

Microsoft has rebranded various Office 365 product lineups as Microsoft 365. The company also announced a new set of personal and family subscriptions for individuals under the new Microsoft 365 name. Microsoft 365 personal and family subscriptions are the company's very first consumer offerings. According to Microsoft, all Office 365 subscriptions for small and medium-sized businesses and the Office 365 ProPlus will use the new Microsoft 365 branding.

Why the change? According to Jared Spataro, corporate vice president for Microsoft 365, this rebranding represents Microsoft's vision for the future of productivity tools. The new service will cost the same but is going to pack some new features and services. Microsoft intends to provide solutions not just for enterprises but also for individuals to help us in everyday lives. And this rebranding aligns Microsoft's vision to "help people and businesses throughout the world realize their full potential," Spataro says.

New product names

Here is the detailed list of products that are now rebranded as Microsoft 365. The company has made it clear that the change is confined to the name only and there is no change in price and feature as of now. However, as mentioned above, Microsoft has plans to introduce a bunch of new features to Microsoft 365's lineup soon.
— *Continued on next page...*

Office 365 Business Essentials is now **Microsoft 365 Business Basic**

Office 365 Business Premium has been rebranded as **Microsoft 365 Business Standard**

Microsoft 365 Business is now called **Microsoft 365 Business Premium**

Office 365 Business and **Office 365 ProPlus** are now **Microsoft 365 Apps**

Microsoft also announced that it will continue to follow the same naming conventions to differentiate its products based on the target audience. For instance, they will continue to use "for business" or "for enterprise" labels wherever necessary to distinguish between the two.

Microsoft 365 personal and family subscriptions

Now that so many people have started to adapt to working remotely due to the ongoing COVID-19 pandemic, Microsoft believes that staying connected is more important than ever. Microsoft announced a whole set of features, products, services, and tools for every individual to help them connect, learn, and achieve more at home.

Microsoft 365 Family and Personal subscriptions are priced at $6.99 monthly or $69 annually for a single user. However, it is just $9.99 monthly or $99 annually for a family subscription of up to six people. This subscription includes all the Microsoft Office apps including Word, PowerPoint, Excel, and more along with all the upcoming new features and apps.

It also offers 1TB of cloud storage space per person or 6TB of storage for a family plan, with each user limited to 1TB. It also includes Microsoft's two new consumer apps called Microsoft Family Safety and Microsoft Teams for consumers. While both these apps are already available in some Microsoft subscriptions, they are now loaded with new features. More information about this new subscription package can be seen here.

Microsoft Family Safety

This app allows users to share their location with family members for safety. This location can be live-tracked by family members or can be set to trigger when they arrive at a predetermined location. It also provides parental controls across various Microsoft products and services including Windows 10, Xbox, and Android.

Microsoft Teams

Microsoft Teams for consumers is a stripped-down version of the enterprise Microsoft Teams, which brings the enterprise communication tool home for family and friends. It comes with group chat feature along with group video calling. It also allows sharing media, making and sharing schedules, events, and more. All these features make it an ideal tool for family events, get-togethers, and sporting events. —*Sukesh Mudrakola for Techgenix*